National Infrastructure Protection Center CyberNotes

Issue #2001-09 *May 7, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between April 6 and May 3, 2001. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Acme Software[1]	Unix	PerlCal 2.13, 2.18, 2.3-2.80, 2.9-2.9e, 2.95	A directory traversal vulnerability exists which could allow a remote malicious user to gain sensitive information.	No workaround or patch available at time of publishing.	PerlCal Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Alex Linde[2]	Windows 95/98/NT 4.0/2000	Alex's Ftp Server 0.7	A directory traversal vulnerability exists which could allow a malicious user to gain sensitive information.	No workaround or patch available at time of publishing.	Alex's Ftp Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Whizkunde Security Advisory, April 27, 2001.
[2] Bugtraq, April 28, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple[3]	MacOS 9.0	MacOS 9.0	A vulnerability exists in the Multiple Users facility, which could allow a malicious user to gain sensitive system information and unrestricted access to the user configuration.	No workaround or patch available at time of publishing.	Apple MacOS Multiple Users Password Bypass	Medium	Bug discussed in newsgroups and websites.
BRS[4]	Windows 95/98/NT 4.0/2000	WebWeaver 0.49beta-0.52beta, 0.60beta-0.62beta	Two vulnerabilities exist: a directory traversal vulnerability and a root path disclosure vulnerability exists when the FTP command 'CD' is submitted augmented by an asterisk character, which could allow a remote malicious user to gain sensitive information.	No workaround or patch available at time of publishing.	WebWeaver FTP Root Path Disclosure and Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploits have been published.
Cisco Systems[5]	Multiple	CBOS 677 Software (C677-I-M), 2.3.0.053, 2.4.1	A console handling vulnerability exists which could allow a malicious user to view sensitive information about the remote router.	No workaround or patch available at time of publishing.	CBOS Show NAT Output Session Switching	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Craig Knudsen[6]	Unix	Web Calendar 0.9.11, 0.9.15-16, 0.9.19-26, 0.9.8	A vulnerability exists due to an input validation error, which could let a remote malicious user execute arbitrary code.	Unofficial Patch (Secure Reality): http://www.secureReality.com.au/patches/WebCalendar-SecureReality.diff	WebCalendar Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
CrossWind [7]	Windows NT, Unix	Cyber Scheduler 2.1	A buffer overflow vulnerability exists in the 'websyncd' daemon, which could let a remote malicious user execute arbitrary code.	Patch available at: http://www.crosswind.com/cybdata.htm	Cyber Scheduler 'websyncd' Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Data Wizard[8]	Windows 95, Unix	WebXQ 2.1.204	A directory traversal vulnerability exists which could allow a malicious user to gain sensitive information.	Upgrade available at: http://www.datawizard.net/Free_Software/WebXQ_Free/webxq_free.htm	WebXQ Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
David Harris[9]	Window NT	Mercury for NetWare prior to 1.48	A buffer overflow vulnerability exists due to inadequate string handling for the APOP authentication command, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.pmail.com/downloads.htm	Mercury for NetWare Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Free Peers Inc.[10]	Windows 95/98/ME	BearShare 2.2-2.2.2	A directory traversal vulnerability exists which could allow a malicious user to gain sensitive information.	Upgrade available at: http://download.cnet.com/downloads/0-1896420-108-69833.html?bt.45605.1857922..dl-69833	BearShare Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[3] Bugtraq, May 3, 2001.
[4] Bugtraq, April 28, 2001.
[5] Securiteam, April 25, 2001.
[6] Secure Reality Pty Ltd. Security Pre-Advisory #4, SRPRE00004, April 24, 2001.
[7] Defcom Labs Advisory, def-2000-18, April 17, 2001.
[8] Securiteam, May 1, 2001.
[9] Securiteam, April 25, 2001.
[10] Securiteam, April 30, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett-Packard[11] ***Patch update[12]***	**Unix**	**HP-UX 10.0.1, 10.10, 10.20, 11.0**	**A Denial of Service vulnerability exists due to improper permissions on some of the files, which could allow a malicious user to gain elevated privileges.**	***The Envizex II and possibly other HP-UX terminals will not work correctly with PHSS_22935 and PHSS_22936. These patches have been withdrawn. Until new patches available, use PHSS_21662 or PHSS_21663. Patches located at: http://itrc.hp.com***	**HP-UX Series 700/800 Asecure Denial of Service**	**Medium**	**Bug discussed in newsgroups and websites.**
Hewlett-Packard[13]	Unix	HP9000 Series 700/800 running HP-UX releases 10.01, 10.10, 10.20, 10.26	A Denial of Service vulnerability exists due to a flaw in the 'PCLToTIFF' program.	**Workaround:** Remove the set group id permissions from 'PCLToTIFF' and allow read access to /usr/lib/ X11/fonts/ifo.st/typefaces/	HP-UX 'PCLToTIFF' Denial of Service	Low	Bug discussed in newsgroups and websites.
Hylafax[14] ***Exploit script published[15]***	**Multiple**	**Hylafax 4.0pl0, 4.0pl1, 4.0pl2, 4.1-beta1, beta2, beta3**	**A format string vulnerability exists in the server binary 'hfaxd,' which could let a malicious user execute arbitrary code.**	**Patch available at: http://www.hylafax.org/patches/hfaxd-vulnerability.patch**	**Hylafax 'hfaxd' Local Format String**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
iPlanet[16]	Windows NT 4.0/2000, Unix	Web Server Enterprise Edition 4.0, 4.1	A buffer overflow vulnerability exists due to improper handling of the response header values, which could let a remote malicious user gain access to sensitive information.	Upgrade available at: http://www.iplanet.com/products/iplanet_web_enterprise/iwsalert4.16.html	Web Server Enterprise Response Header Overflow	Medium	Bug discussed in newsgroups and websites.
IpSwitch[17]	Windows NT 4.0/2000	IMail 6.0-6.0.6	A vulnerability exists due to improper bounds checking in the IMAIL SMTP daemon, which could let a remote malicious user gain system level access and execute arbitrary code.	Patch available at: http://ipswitch.com/support/IMail/patch-upgrades.html	IMail SMTP Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
KDE[18]	Unix	kdelibs 2.0-2.1.1	A vulnerability exists in the 'kdesu' program, which could let a malicious user gain elevated privileges and compromise the account accessed by kdesu.	Update available at: ftp://updates.redhat.com/7.1/en/os/i386	KDE kdesu Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites.

[11] Hewlett-Packard Company Security Bulletin, HPSBUX0103-145, March 7, 2001.
[12] Hewlett-Packard Company Security Bulletin, HPSBUX0103-145 Rev 2, April 6, 2001
[13] Hewlett-Packard Company Security Advisory, HPSBUX0104-149, April 19, 2001.
[14] Securiteam, April 12, 2001.
[15] Securiteam, April 24, 2001.
[16] @stake Security Advisory, A041601-1, April 17, 2001.
[17] eEye Digital Security Advisory, April 24, 2001.
[18] Red Hat Security Advisory, RHSA-2001:059-03, April 30, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Max Feoktistov [19]	Windows 95/98	Small HTTP server 2.03	A remote Denial of Service vulnerability exists when a URL request for an MS-DOS devicename is submitted.	No workaround or patch available at time of publishing.	Small HTTP Server MS-DOS Device Name Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft [20]	Windows 2000	Windows 2000 Server, Professional Server, Datacenter Server, Advanced Server	An unchecked buffer overflow vulnerability exists in 'msw3prt.dll,'which could let a malicious user execute arbitrary code. Note: The vulnerability is only exposed if IIS 5.0 is running.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-023.asp	Microsoft Windows 2000 IIS 5.0 IPP ISAPI 'Host:' Buffer Overflow CVE Name: CAN-2001-0241	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published. Vulnerability has appeared in the Press and other public media.
Microsoft [21]	Windows 95/98/NT 4.0/2000	Outlook Express 5.0, 5.5; Internet Explorer 5.0, 5.5	It is possible to execute Active Scripting with the help of XML and XSL even if Active Scripting has been disabled in all security zones. This is especially dangerous in e-mail messages.	Microsoft has addressed this issue in a patch originally for a Windows Script Host issue, which is available at: http://www.microsoft.com/technet/security/bulletin/MS01-015.asp	Microsoft IE and OE XML Stylesheets Active Scripting		Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft [22] ***Microsoft rereleases patch*** [23]	**Windows 95/98/NT 4.0/2000**	**Internet Explorer 5.01, 5.5; Windows Scripting Host 5.1, 5.5**	**A vulnerability exists in IE and Windows Scripting Host that could let a malicious user execute arbitrary code.** ***A regression error was found in the previously released Windows Script Host patch. The re-release only applies to changes with the Windows Script Host patches.***	***Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-015.asp***	**Internet Explorer and Windows Scripting Host Cached Location** **CVE name: CAN-2001-0002**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Microsoft [24]	Windows 95/98/NT 4.0/2000, Apple MacOS 7.0-7.1.2, 7.5.1-7.6.1, 8.0, Unix	Windows Media Player 6.3, 6.4, 7	A vulnerability exists in the Active Stream Redirector (ASX) component, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Windows Media Player .ASX Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Mirabilis [25]	Windows 95/98/ME/ NT 4.0/2000	ICQ 2000.0b Build 3278	A remote Denial of Service vulnerability exists due to the handling of unusual input in a GET request.	No workaround or patch available at time of publishing.	ICQ Web Front Plug-In Denial of Service	Low	Bug discussed in newsgroups and websites.

[19] Bugtraq, April 24, 2001.
[20] Microsoft Security Bulletin, MS01-023, May 1, 2001.
[21] Georgi Guninski Security Advisory #43, April 20, 2001.
[22] Microsoft Security Bulletin, MS01-015, March 6, 2001.
[23] Microsoft Security Bulletin, MS01-015 version 2.0, April 20, 2001.
[24] Bugtraq, May 2, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla [26]	Windows 95/98/NT 3.5.1/4.0	Bugzilla 2.10, 2.4, 2.6, 2.8	A vulnerability exists in the file, 'globals.pl', which could let a malicious user gain sensitive information.	Upgrade available at: http://ftp.mozilla.org/pub/webtools/bugzilla-2.12.tar.gz	Bugzilla Sensitive Information Disclosure CVE Name: CAN-2001-0330	Medium	Bug discussed in newsgroups and websites. No exploit is required.
Mozilla [27]	Windows 95/98/NT 3.5.1/4.0	Bugzilla 2.10, 2.4, 2.6, 2.8	A vulnerability exists because user e-mail addresses are not checked for shell meta-characters, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://ftp.mozilla.org/pub/webtools/bugzilla-2.12.tar.gz	Bugzilla Remote Arbitrary Command Execution CVE Name: CAN-2001-0329	**High**	Bug discussed in newsgroups and websites. No exploit is required.
Multiple Vendors [28, 29, 30]	Unix	gFTP 0.1-2.0.7; Red Hat Linux 6.2 - alpha, i386, sparc, 7.0 - alpha, i386, 7.1 - i386; Linux Mandrake 7.1, 7.2, 8.0, Corporate Server 1.0.1; Immunix OS 6.2, 7.0-beta, 7.0	A format string vulnerability exists in the facility used by the gftp client program to log FTP and HTTP responses, which could let a remote malicious user execute arbitrary code.	**RedHat:** ftp://updates.redhat.com **LinuxMandrake:** http://www.linux-mandrake.com/en/ftp.php3 **Immunix:** http://immunix.org/ImmunixOS/	gFTP Remote Format String	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors [31, 32, 33]	Unix	NEdit 5.5.1	A temporary file vulnerability exists in NEdit (Nirvana Editor), which could let a malicious user gain access to other user privileges including root.	**LinuxMandrake:** http://www.linux-mandrake.com/en/ftp.php3 **Debian:** http://security.debian.org/dists/stable/updates/non-free/ **Progeny:** http://archive.progeny.com/progeny/updates/newton/	NEdit Incremental Backup File Symbolic Link	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
NetCruiser Software [34]	Windows 95/98/NT 4.0/2000	NetCruiser Web Server 0.1.2.8	A vulnerability exists when a requested URL is appended with a specific device name, which could allow a remote malicious user to gain access to the root directory path.	No workaround or patch available at time of publishing.	NetCruiser Software NetCruiser Web Server Path Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[25] Strumpf Noir Society Advisories, April 28, 2001.
[26] @stake Security Advisory, A043001-1, April 30, 2001.
[27] @stake Security Advisory, A043001-1, April 30, 2001.
[28] Red Hat Security Advisory, RHSA-2001:053-06, April 25, 2001.
[29] Linux-Mandrake Security Update Advisory, MDKSA-2001:044, April 27, 2001.
[30] Immunix OS Security Advisory, IMNX-2001-70-017-01, April 27, 2001.
[31] Linux-Mandrake Security Update Advisory, MDKSA-2001:042, April 25, 2001.
[32] Debian Security Advisory, DSA-053-1, April 27, 2001.
[33] Progeny Service Network Security Advisory, PROGENY-SA-2001-10, April 27, 2001.
[34] Bugtraq, April 24, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Netopia[35]	MacOS	Timbuktu Preview for Mac OS X	A security vulnerability exists which could let a malicious user gain complete access to the system without even having to log into the Mac OS X.	No workaround or patch available at time of publishing.	Timbuktu Mac OS X Login	**High**	Bug discussed in newsgroups and websites.
Netscape[36] ***Vulnera-blity appears in Press[37]***	**Windows 95/98/NT 4.0/2000, Unix**	**Netscape Smart Download 1.3**	**A buffer overflow vulnerability exists in the 'sdph20.dll' library, which could let a malicious user execute arbitrary code or gain administrative privileges.**	**Upgrade available at: http://home.netscape.com/download/smartdownload.html**	**Smart Download Buffer Overflow** **CVE Name: CAN-2001-0262**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.** ***Vulnerability has appeared in the Press and other public media.***
Novell[38]	Multiple	Border Manager 3.0-3.6; Border Manager Enterprise Edition 3.5	A Denial of Service vulnerability exists when numerous TCP SYN packets are sent to port 353.	Patch available at: http://support.novell.com/servlet/filedownload/pub/bmvpn3x.exe	Border Manager Remote Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. Exploit script has been published.
PhpMy Admin Develop-ment Team[39]	Unix	PhpMy Admin 2.1.0, 2.2.1	A vulnerability exists due to the insufficient validation of input by the sql.php script, which could allow a remote malicious user to execute arbitrary code.	Patch available at: ftp://ftp.greatbridge.org/pub/phppgadmin/stable/phpPgAdmin_2-3.tar.gz	phpMyAdmin and phpPgAdmin Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
PhpSecure Pages Develop-ment Team[40]	Unix	PhpSecure Pages 0.23 beta	A security vulnerability exists which could allow a remote malicious user to execute arbitrary code.	Unofficial patch (SecureReality): http://www.secureReality.com.au/patches/phpSecurePages-SecureReality.diff	PhpSecure Pages Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
RedHat[41]	Unix	Linux 7.1	A vulnerability exists in the creation of swap files, which could allow a malicious user to gain sensitive information.	Upgrade available at: ftp://updates.redhat.com/7.1/en/os/	Linux Swap File World Readable Permissions	Medium	Bug discussed in newsgroups and websites.
RedHat[42]	Unix	RedHat 6.2	A vulnerability exists in 'mkpasswd' random password generation function that causes the program to generate relatively simple passwords.	No workaround or patch available at time of publishing.	'mkpasswd' command Cryptographic Generation	Medium	Bug discussed in newsgroups and websites.

[35] Securiteam, April 19, 2001.
[36] @stake Security Advisory, A041301-1, April 13, 2001.
[37] The Register, April 24, 2001.
[38] Bugtraq, April 20, 2001.
[39] Secure Reality Pty Ltd. Security Pre-Advisory #1, SRPRE00001, April 24, 2001.
[40] Secure Reality Pty Ltd. Security Pre-Advisory #2, SRPRE00002, April 24, 2001.
[41] Red Hat Security Advisory, RHSA-2001:058-04, May 2, 2001.
[42] Securiteam, April 12, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Rit Research Labs[43]	Windows 95/98/NT 4.0	The Bat! 1.011-1.5.1	A remote Denial of Service vulnerability exists when retrieving a message via POP3.	No workaround or patch available at time of publishing.	The Bat! Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
RobTex[44]	Windows 95/98/NT 3.5.1/4.0/ 2000	Viking Server 1.0.4-1.0.7	A directory traversal vulnerability exists due to improper handling of relative paths, which could allow a remote malicious user to gain sensitive information.	Upgrade available at: ftp://ftp.robtex.com/robtex/viking/vslatest.zip	Viking Server Relative Path Webroot Escaping	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SAP[45]	Unix	Saposcol for Linux 1.0-1.3	An input validation vulnerability exists in the SAP Operating System Collector (saposcol), which could let a malicious user execute arbitrary code.	Upgrade available at: Ftp://ftp.sap.com/pub/linuxlab/saptools/saposcol	SAP Web Application Server for Linux Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Sendfile[46]	Unix	Sendfile 1.4-1.6, 2.1	A vulnerability exists in the Sendfile asynchronous file transfer daemon, which could let a malicious user execute arbitrary code and gain 'group 0' privileges. If exploited, this would be a complete system compromise.	**Debian:** http://security.debian.org/dists/stable/updates/main/ **Sendfile:** ftp://ftp.belwue.de/pub/unix/sendfile/current/sendfile-20010216.tar.gz	Sendfile Local Privileged Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. No exploit script is required.
Sendfile[47]	Unix	Sendfile 1.4-1.6, 2.1	A serialization error exists in the 'sendfiled,' which could let a malicious user execute arbitrary commands as root and gain elevated privileges.	Upgrade available at: ftp://ftp.belwue.de/pub/unix/sendfile/current/sendfile-20010216.tar.gz	Sendfile Forced Privilege Lowering Failure	**High**	Bug discussed in newsgroups and websites.
Silicon Graphics Inc.[48]	Unix	IRIX 5.3, 6.0- 6.5.9	A vulnerability exists in the –n option, which could allow a malicious user to execute arbitrary code and gain root access.	No workaround or patch available at time of publishing.	IRIX 'netprint' Arbitrary Shared Library Usage	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Spencer Christensen[49]	Unix	Perl Web Server 0.0.1-0.0.4, 0.1-0.3	A directory traversal vulnerability exists which could allow a remote malicious to gain sensitive information.	No workaround or patch available at time of publishing.	Perl Web Server Path Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Micro Systems, Inc.[50]	Unix	Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the –F option, which could let a malicious user gain elevated privileges.	Unofficial workaround (Bugtraq): Remove the setGID bit from the /bin/mailx program.	Solaris Mailx -F Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.

[43] Bugtraq, April 18, 2001.
[44] Bugtraq, April 23, 2001.
[45] Bugtraq, April 30, 2001.
[46] Debian Security Advisory, DSA 052-1, April 23, 2001.
[47] Progeny Linux Systems, PROGENY-SA-2001-08, April 20, 2001.
[48] Securiteam, May 2, 2001.
[49] Bugtraq, April 24, 2001.
[50] Bugtraq, May 2, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Team JohnLong[51]	Windows ME/98/NT 4.0/2000	RaidenFTPD 2.1 build 947-951	A directory traversal vulnerability exists which could allow a malicious user to gain sensitive information.	Upgrade available at: http://playstation2.idv.tw/raidenftpd/download.html	RaidenFTPD Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Tektronix[52]	Multiple	Phaser Network Printer 740, 750, 750DP, 850, 930	A remote vulnerability exists which could let a malicious user access the printer's local network and reach the admin interface. The printer's 'Emergency Power Off' feature can be activated, which could lead to physical damage to the device.	No workaround or patch available at time of publishing.	Phaser Network Printer Administration Interface	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Texas Imperial Software[53]	Windows NT 4.0	WFTPD 3.00R4 Pro, WFTPD 3.00R4	A buffer overflow vulnerability exists in the 'RETR' and 'CWD' commands, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.wftpd.com/	WFTPD 'RETR' and 'CWD' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
The Net[54]	Windows 95/98/NT 4.0	CheckBo 1.56	A remote Denial of Service vulnerability exists due to a buffer overflow when invalid input is submitted to the service listening on TCP ports 54320, 20034, 12345, 12346, 31337, 31666, 1243, and 6713.	No workaround or patch available at time of publishing.	CheckBo Denial of Service	Low	Bug discussed in newsgroups and websites.
Trend Micro[55]	Windows NT	ScanMail for Exchange version 3.5	A vulnerability exists in the Management Console that could let a malicious user compromise the administrative account.	**Workaround:** Trend Micro recommends, as a temporary fix, that the following keys (and all sub-keys) should have their permissions set to Full Control for Administrators and SYSTEM (remove all other permissions): HKLM \Software\TrendMicro\ScanMail for Exchange \RemoteManagement HKLM \Software\TrendMicro\ScanMail for Exchange \UserInfo	ScanMail Insecure Password Storage	**High**	Bug discussed in newsgroups and websites.

[51] Bugtraq, April 25, 2001.
[52] Bugtraq, April 25, 2001.
[53] Bugtraq, April23, 2001.
[54] Bugtraq, April 20, 2001.
[55] Securiteam, April 26, 2001.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such a vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of a medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 17, and May 3, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 29 scripts, programs, and net-news messages containing holes or exploits were identified.
NOTE: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 3, 2001	Mimedefang-1.1.tar.gz	A flexible MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables.
May 2, 2001	Iishack2000.c	Script which exploits the Windows 2000 / IIS 5.0 sp0 + sp1 Internet Printing Protocol vulnerability.
May 2, 2001	Jill.c	Perl script which exploits the Windows 2000 / IIS 5.0 sp0 + sp1 Internet Printing Protocol vulnerability.
May 2, 2001	**Mailx-F.c**	**Script which exploits the Solaris mailx -F Buffer Overflow vulnerability.**
May 2, 2001	**Moneyiswrong.asx**	**Exploit for the Windows Media Player .ASX Buffer Overflow vulnerability.**
May 2, 2001	Webexplt.pl	Perl script which exploits the Windows 2000 / IIS 5.0 sp0 + sp1 Internet Printing Protocol vulnerability.
April 30, 2001	Border.c	Script which exploits the Novell BorderManager Enterprise remote Denial of Service vulnerability.
April 30, 2001	Ettercap-0.4.2.tar.gz	A network sniffer for switched LANs, which uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts.
April 30, 2001	Intro_to_arp_spoofing.pdf	Introduction to Arp Spoofing, a method of exploiting the interaction between IP and Ethernet protocols. Includes discussion of switched sniffing, man-in-the middle attacks, hijacking, cloning, poisoning and more.
April 30, 2001	**Perlcal.txt**	**Exploit URL for the PerlCal Directory Traversal vulnerability.**
April 30, 2001	Sara-3.4.1.tar.gz	A security analysis tool based on the SATAN model.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
April 30, 2001	Squirtv1.2.tar.gz	Perl tool for finding and exploiting local buffer overflow vulnerabilities.
April 30, 2001	Tfak5.zip	Trojan scanner that detects 736 remote access Trojans and 9 file joiners.
April 30, 2001	**Xnetprint.c**	**Script which exploits the Irix Netprint vulnerability.**
April 27, 2001	Tcpip_lib31.zip	A library for Windows 2000, which allows IP construction, IP spoofing attacks, and more.
April 25, 2001	Hfaxd-fs-exploit.pl	Perl script which exploits the Hylafax (/usr/libexec/fax/hfaxd) format string vulnerability.
April 24, 2001	Ezpass.zip	Perl script that uses the net command to automate password attempts on an NT Server.
April 24, 2001	Grinder.zip	An executable and Perl script that uses the SID tools to enumerate usernames from an NT Server.
April 24, 2001	Hexyn-sa-19.txt	Perl exploit for the FTP Server Denial Of Service vulnerability.
April 23, 2001	7350cfingerd-0.0.4.tar.gz	Script that exploits the Cfingerd format string vulnerability.
April 23, 2001	Ngrep-1.39.2.tar.gz	A network sniffing tool which strives to provide most of GNU grep's common features, applying them to all network traffic.
April 23, 2001	Talkbackcgi-exp.pl	Perl script which exploits the TalkBack.cgi directory traversal vulnerability.
April 23, 2001	Wftpdsploit.c	Script which exploits the WFTPD 'RETR' and 'CWD' Buffer Overflow vulnerability.
April 22, 2001	Cheops-ng-0.1.4.tgz	A graphical network management tool for mapping and monitoring your network, which does a port scan.
April 22, 2001	Saint-3.1.4.tar.gz	An updated version of SATAN designed to assess the remote security of computer networks.
April 22, 2001	Sing-1.1.tar.gz	A tool that sends ICMP packets fully customized from the command line. Its main purpose is to replace and complement the ping command, adding certain enhancements as fragmentation, sending and receiving spoofed packets, sending many ICMP information types.
April 20, 2001	Xstyle.eml	Exploit for the Microsoft IE and OE XML Stylesheets Active Scripting vulnerability.
April 18, 2001	**Badmess.zip**	**Exploit for the Rit Research Labs The Bat! Missing Linefeeds Denial of Service vulnerability.**
April 17, 2001	X-cybersched.c	Script which exploits the CrossWind Cyber Scheduler websyncd remote Buffer Overflow vulnerability.

Trends

Probes/Scans:

There has been an increase in the number of scans and attacks to port 515 looking for the LPRng User-Supplied Format String vulnerability, Wu-Ftpd Remote Format String Stack Overwrite Vulnerability, ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability, and the rpc.statd Remote Format String Vulnerability.

Other:

CERT/CC has received reports of a new piece of self-propagating malicious code referred to as the sadmind/IIS worm (for more information, see Virus Section). The worm uses two well-known vulnerabilities to compromise systems and deface web pages. A two-year-old buffer overflow vulnerability in the Solstice sadmind program, and after successfully compromising the Solaris systems, it uses a seven-month-old vulnerability to compromise the IIS systems. For more information, please see CERT® Advisory CA-2001-11, located at: http://www.cert.org/advisories/CA-2001-11.html.

CERT/CC has received reports that a distributed denial-of-service (DDoS) tool named Carko is being installed on compromised hosts. For more information, please see CERT® Incident Note IN-2001-04, located at: http://www.cert.org/incident_notes/IN-2001-04.html.

The NIPC has received reliable information indicating ongoing attempts to disrupt web access to several sites. The activity has been seen from several networks, and consists entirely of fragmented large UDP packets directed at port 80. For more information, please see NIPC Advisory 01-012, located at: http://www.nipc.gov/warnings/advisories/2001/01-012.htm.

The NIPC has received information concerning a new version of the "lion" worm that has been reported to be attempting to infect computers. This new version appears to be similar to past versions, with the exception that it retrieves a rootkit from a new address. For more information, please see NIPC Advisory 01-005 Update, located at: http://www.nipc.gov/warnings/advisories/2001/01-005.htm.

There has been a very significant increase in attempts to exploit known weaknesses in the lpd/LPRng and RPC daemons (ports 515 and 111) of Unix-based operating systems. For more information, please see NIPC ALERT 01-010, located at: http://www.nipc.gov/warnings/alerts/2001/01-010.htm.

The NIPC has issued an advisory concerning an unchecked buffer vulnerability in an Internet Service Application Program Interface (ISAPI) extension that could allow the compromise of an IIS 5.0 web server. For more information, please see NIPC ADVISORY 01-011, located at: http://www.nipc.gov/warnings/advisories/2001/01-011.htm.

NIPC has issued an advisory concerning a potential security vulnerability that exists in PDG Software, Inc. Shopping Cart software (versions prior to 1.63) which is being actively exploited. For more information, please see NIPC ADVISORY 01-007, located at: http://www.nipc.gov/warnings/advisories/2001/01-011.htm, or Microsoft Security Bulletin MS01-023, located at: http://www.microsoft.com/technet/security/bulletin/MS01-023.asp.

Several Microsoft Hotfixes downloaded between April 6-20 from Microsoft's Premium Support and Gold Certifies Web sites were infected with PE_FUNLOVE.4099 (a.k.a. "the Fun Love virus"). (See the Virus Section for additional information).

Numerous reports have been received indicating that the snmpXdmid vulnerability is actively being exploited which could allow a malicious user to gain root access. For more information, please see CERT® Advisory CA-2001-05, located at: http://www.cert.org/advisories/CA-2001-05.html.

Worms are being released based on well-known exploits such as Bind, LPRng, rpc-statd, and wu-ftpd. A software package has been released which, if used maliciously, may disable a victim's computer or network's IDS by flooding it with Internet traffic emanating from several random Internet Protocol (IP) addresses simultaneously. For more information, please see NIPC ASSESSMENT 01-004, located at: http://www.nipc.gov/warnings/assessments/2001/01-004.htm.

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available.
NOTE: At times, viruses may contain names or content that may be considered offensive.

PE_FUNLOVE.4099 (Aliases: W32/FUNLOVE, FUNLOVE.4099) (File Infector Virus): This virus has been reported in the wild. Upon execution, the virus drops the file FLCSS.EXE in the Windows System Folder. It then infects all EXE, SCR, and OCX files in the Program Files folder, including sub folders. While EXPLORER.EXE is in memory, the virus re-executes at every system startup. In addition, because EXPLORER.EXE and other system files execute when Windows is loaded, the virus cannot be cleaned in Windows. The virus attaches the FLCSS.EXE file at the end of the last section of infected files. For it to execute and jump directly to the entry point of the FLCSS.EXE attachment, it modifies the entry point of the host file. In an NT environment, this virus patches the integrity checking of NTOSKRNL by modifying the NTLDR file (found in the root directory). The virus then modifies the NTOSKRNL (in the

\WINNT\SYSTEM32 directory) and disables the access-rights checking. It then infects system files. Note: Several Microsoft Hotfixes downloaded between April 6-20 from Microsoft's Premium Support and Gold Certifies Web sites were infected with PE_FUNLOVE.4099.

Sadmind-IIS (Alias: sadmind/IIS) (Self-propagating Worm): This worm affects both:

Systems running unpatched versions of Microsoft IIS
Systems running unpatched versions of Solaris up to, and including, Solaris 7

The sadmind-IIS worm exploits a known vulnerability in unpatched Solaris systems. The worm installs software to attack Microsoft IIS web servers. Afterwards, it attempts to propagate itself to other vulnerable Solaris systems. Compromised Solaris systems will have "+ +" added to the rhosts file in the root user's home directory. Also, the index.html on the host Solaris system will be modified. Solaris systems compromised by this worm are being used to scan and compromise other Solaris and IIS systems. IIS systems compromised by this worm can suffer modified web content. Intruders can use the vulnerabilities exploited by this worm to execute arbitrary code with root privileges on vulnerable Solaris systems, and arbitrary commands with the privileges of the IUSR_machinename account on vulnerable Windows systems.

VBS_CHALLENGE.A (Aliases: VBS.CHALLENGE, CHALLENGE.A) (Visual Basic Script Worm): This worm propagates via e-mail in Microsoft Outlook Express. It embeds itself as a script program in Visual Basic Script language in the messages it sends.

VBS.Gift.Int (Visual Basic Script Worm): This is a worm written in the Visual Basic Scripting language. It attempts to send itself to all addresses in your Microsoft Outlook Address Book. However, due to a bug or corruption in the code of VBS.Gift.Int, the worm does not work as intended, and it appears to be unable to spread its infection.

VBS_HOMEPAGE.A (Aliases: HOMEPAGE.A, VBS/VBSWG.X, VBS/VBSWG.X@mm, VBS.VBSWG2.D@mm, VBS/SSI.gen@MM, VBS/SSI.gen, SSI, VBSWG) (Visual Basic Script Worm): This Internet worm has been reported in the wild. It was created with a Visual Basic Script worm generator, vbswg2.x. In order for the worm to execute, it requires the Windows Scripting Host to be installed. Upon execution, it drops a copy of itself in the Windows directory as :HOMEPAGE.HTML.VBS." The worm then checks for the following registry entry to see if an e-mail has already been sent out to all addresses in the address book:

HKCU\Software\An\Mailed

If the entry has the value 1, it means the worm has propagated, otherwise, the worm sends itself out as an attachment to all addresses listed in the MS Outlook address book of the infected user and then creates the above registry entry with a value 1. If the infected system does not have MS Outlook, the worm cannot propagate. After sending out an e-mail, the worm tries to randomly open the following pornographic Web sites with Internet Explorer:

http://hardcore.pornbillboard.net/shannon/1.htm
http://members.nbci.com/_XMCM/prinzje/1.htm
http://www2.sexcropolis.com/amateur/sheila/1.htm
http://sheila.issexy.tv/1.htm

The worm then checks if the e-mail that it sent out exists in the MS Outlook Journal and Sent Items folder by looking for the subject "Homepage." When it finds AN e-mail with the subject "Homepage" in these folders, the worm deletes the e-mail to prevent detection.

VBS.Gorum.A@mm (Alias: VBS/Gorum.gen@MM) (Visual Basic Script Worm): This is an encoded Visual Basic Script (VBE) worm. It arrives as the attachment STU-CMH.txt.vbe. Like many other worms, it uses Microsoft Outlook to spread. The worm deletes multiple files and folders from drives C through F.

VBS.Ketip.B@mm (Aliases: I-Worm.SSIWG.e VBS/Gorum.gen@MM) (Visual Basic Script Worm): This is a Visual Basic Script (VBS) worm. It arrives as the attachment Judge.TXT.vbs and uses Microsoft Outlook to spread. The script attempts to connect to an FTP server and download a program, which might be malicious.

VBS/San-B (Visual Basic Script Worm): This is a variant of VBS/San-A worm that uses the file 'LOVEDAY14-C.HTA' instead of 'LOVEDAY14-B.HTA'.

VBS.vbswg2.C@mm (Visual Basic Script Worm): This worm is a Visual Basic Script (VBS) worm that uses Microsoft Outlook to spread. It sends itself to all addresses in the Microsoft Outlook address book. VBS.vbswg2.C@mm arrives as:

Subject: this e-card for you. (WWW.é-card.com).
Message: The message body is empty.
Attachment: e-card.vbs

It also spreads using mIRC and PIRCH. This worm creates many files on the system. It also may change your Microsoft Internet Explorer home page to a page hosted by Geocities. This page appears to have been removed.

W32.Stator@mm (W32 Worm): W32.Stator@mm is a mass-mailing worm program. It renames specific Windows programs so that they have a file extension of .vxd, and it then uses the original file names for duplicate copies of the worm itself.

W97M_LISTI.A (Alias: LISTI.A) (Word 97 Macro Virus): When a document is opened, this Word macro virus infects other active documents. Upon execution, this macro virus overwrites its viral code to the contents of the ThisDocument module, and NORMAL.DOT of the global template. The virus resets its values in the registry to disable the macro virus protection (Windows 2000 and XP only). If the system time contains the number 5, it runs the Agent application (Office assistant) and then displays a series of messages. It carries no destructive payload.

W97M.Rendra.D.Gen (Aliases: Macro.Word.97.Rendra.b, W97M/Rendra.gen) (Word 97 Macro Virus): When an infected document is opened, the macro virus will infect active documents and the Normal.dot template by rewriting the following auto macros (if they exist) in the ThisDocument macromodule: AutoNew, AutoOpen, AutoClose

W97M.Sunirt.A.Gen (Word 97 Macro Virus): This is a macro virus that infects active documents and the Normal.dot template file. The virus also creates duplicates of infected documents, and saves the copies in the C:\My Documents folder, using the user name as the file name.

WM97/Hope-AC (Word 97 Macro Virus): This is a simple Word macro virus, which may remove 'Macros' and 'Options' from the Tools menu.

WM97/Metys-F (Word 97 Macro Virus): This is a minor variant of the WM97/Metys-D Word macro virus. This variant of the virus spreads but does not have a working payload.

X97M.Pink.A.Gen (Excel 97 Macro Virus): This virus is a variant of the X97M/Laroux virus. When a worksheet that is contained in a X97M.Pink.A.Gen infected workbook is opened, the virus adds a copy of the infected workbook to the \XLStart folder as the BOOK1.xls file. The BOOK1.xls file then infects all clean workbooks when any worksheet is opened. If the sum of the current month and the current date is 13 or 22, then it will protect the active worksheet with a random 8-digit password. If the current date is June 15, it will change the format and contents of the active worksheet cells so that a large "swastika" symbol is displayed.

X97M.Squared.B.Gen (Excel 97 Macro Virus): On opening a X97M.Squared.B.Gen infected workbook, the virus adds a copy of the infected workbook to the \XLStart folder as the Nt2.xls file. The Nt2.xls file then infects all clean workbooks when they are opened.

Zag.1106 (DOS Virus): This is a DOS .exe virus. Damage done by the virus is not repairable. It writes its viral code onto all files that are in the same folder as the virus, as well as in the root directory.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects.
NOTE: At times, Ttrojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-JZ	N/A	CyberNotes-2001-02
BAT.Install.Trojan	N/A	CyberNotes-2001-04
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
Fatal Connections	**2.0**	**Current Issue**
Flor	N/A	CyberNotes-2001-02
Freddy	**beta 3**	**Current Issue**
Gift	**1.6.13**	**Current Issue**
HardLock.618	N/A	CyberNotes-2001-04
JS.StartPage	N/A	CyberNotes-2001-07
Noob	**4.0**	**Current Issue**
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
SadCase.Trojan:	**N/A**	**Current Issue**
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
Troj/Unite-C	**N/A**	**Current Issue**
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_FUNNYFILE.A	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HAVOCORE.A	**N/A**	**Current Issue**
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_INCOMM16A.S	**N/A**	**Current Issue**
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_LASTWORD.A	**N/A**	**Current Issue**
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MTX.A.DLL	**N/A**	**Current Issue**
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NARCISSUS.A	**N/A**	**Current Issue**
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Lumorg	**N/A**	**Current Issue**
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS_HAPTIME.A	**N/A**	**Current Issue**
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07

Fatal Connections (2.0): This is a Visual Basic 6 Trojan. It is one of the few Trojans that can speak on infected computers. The Trojan uses a text 2 speech engine to allow whatever the perpetrator types to be spoken from your speakers. However, this feature requires a system extra system file, which makes infecting people with this Trojan more difficult.

Freddy (beta 3): This is a German Trojan that has an edit server program and allows an e-mail address to be notified when the infected computer comes online.

Gift (1.6.13): This is a Visual Basic remote access Trojan. The Trojan needs imgedit.ocx to run, which is an uncommon file making infection more difficult. Also, when the server is run, it displays a box saying "you are infected with the Gift Trojan," which makes it hard to be infected with this Trojan without knowing it.

Noob (4.0): This is an Active X Trojan. The Trojan is imbedded in an actual htm file. Noob 4.0 works on Internet Explorer 5.0 and some versions of 5.5. When the page is viewed with Internet Explorer, you must say yes to an Active X question or else the Trojan will not install. Unlike the pervious versions of Noob, this version has a wizard program to create the htm file. This wizard program allows a second file, which could be another Trojan or virus, to be embedded in the htm file.

SadCase.Trojan: This is an extremely destructive Trojan horse written in Visual C++. When run, it immediately starts to delete all files and folders on drive C. It deletes files by using the DOS command "deltree /y C:\" so that all files and folders are deleted from drive C without asking the user for confirmation. While deleting files, it displays two dialog boxes. Once these messages are displayed, it is probably too late to turn your computer off and save your data. Also, SadCase.Trojan inserts the batch file C:\Windows\Start Menu\Programs\StartUp\Owned.bat, which displays a taunting message the next time the computer is started. This message is only displayed if the Owned.bat file still exists and the operating system is still functioning.

TROJ_FUNNYFILE.A (Aliases: FUNNYFILE.A, W32.FunnyFile.worm, W32.Hello.worm): This non-destructive Trojan is designed to propagate via e-mail. However, due to some errors in its code it is unable to execute the routine that allows the Trojan to propagate.

TROJ_HAVOCORE.A (Alias: HAVOCORE.A): This server side of a backdoor Trojan allows a remote user access to an infected system, compromising network security. Upon execution, this Trojan drops a copy of itself as MSCLOP.EXE in the Windows directory. It arrives with a stealth mechanism to delete its original copy after execution and adds a registry entry in the Windows run directory so that its dropped file executes when Windows restarts. The features incorporated in the client side of this hacking tool identify the different manipulations that may be performed on an infected system.

TROJ_INCOMM16A.S (Aliases: Incommand 1.6.5 Srv 16, BackDoor-DB.svr.gen, INCOMM16A.S): This backdoor Trojan allows a remote user access to an infected system and disguises itself as a System Security Control and Network Monitor program. It may be circulated as MSSECURE.EXE. It is a memory resident Trojan that is comprised of a server side and a client side. The server side is installed to infect a target computer. The client side of this Trojan provides a User Interface (UI) to connect to an infected system. The remote hacker specifies an Internet Protocol address of an infected system and the Transmission Control Protocol (TCP) port 9400 where the server operates. It compromises network security.

TROJ_LASTWORD.A (Aliases: I-Worm.LastWord, WinUpdate, LASTWORD.A): This Trojan e-mails itself as an attachment to all entries in an infected user's MS Outlook address list. When a system is already infected, it displays different messages at every boot up. It drops an OPOMENA.TXT file that contains a counter that the Trojan uses to count the number of times its infected system is booted.

TROJ_MTX.A.DLL (Alias: MTX.A.DLL): This Trojan infects WIN32 files in the current directory and propagates via e-mail as an attachment. Another virus, PE_MTX.A, infects the attached file and then

installs a backdoor application in the infected system. The Trojan copies the WSOCK32.DLL to the system directory as WSOCK32.MTX and then patches the Send() function that intercepts SMTP to modify WSOCK32.DLL. If the Trojan fails, it modifies WSOCK32.MTX instead, and inserts an entry in the WININIT.INI infecting WSOCK32.DLL. Thereafter, the Trojan can monitor when an infected system accesses the Internet and sends e-mails. It prevents an infected user from accessing antivirus sites and sending messages to certain e-mail servers.

TROJ_NARCISSUS.A (Aliases: NARCI.WORM, NARCISSUS.A, HAPPY NEW YEAR WORM, LEILALOVE.WORM): This Trojan propagates via e-mail, and is disguised as a wallpaper installation program. It arrives as an e-mail attachment, NARCISSUS.EXE, with a heart icon. It carries no destructive payload. Upon execution, it drops two files, NARCI.JPG and NARCI.EXE, in the \WINDOWS\TEMP\L\ NARCISSUS folder. It then executes NARCI.EXE, which contains the e-mailing procedure in Microsoft Outlook that sends e-mails to all entries in the infected user's address list. It arrives in an e-mail with the following:

Subject: Happy new year ;-)
Message Body: Run and see nice wallpaper
Attachment: NARCISSUS.EXE

NARCI.JPG is set as the default wallpaper so that it hides the execution of the Trojan file

Troj/Unite-C: This Trojan has been reported in the wild. It is a configurable, password-stealing program from Russia. The name of the Trojan file is one of the configurable options, so it will change. When run, this file may copy itself to the Windows system directory and add a new key to the Registry containing the path to the file. The Trojan may stay resident and monitor the system, or simply run once on restart. In either case it will establish a TCP port connection to try to send out the stolen information.

VBS.Lumorg (Alias: VBS.Lucky2) (Visual Basic Script Trojan): This is a Visual Basic Script Trojan horse. If the virus is executed, it overwrites all files that are located in the same folder as itself. It also adds the link http://the-myth.iwarp.com to Internet Explorer's Favorites menu. The link appears on the menu as "Morglum." It then starts Internet Explorer and connects to the Web site.

VBS_HAPTIME.A (Aliases: VBS/Helper, HAPTIME.A): This Visual Basic Script (VBS) Trojan propagates via MS Outlook as an attachment called UNTITLED.HTM. It changes an infected user's active wallpaper. It carries two payloads: deleting .EXE and .DLL files and sending or forwarding e-mails to all addresses listed in an infected user's address book. It executes its payloads when the month number plus the day equals 13, and after the Trojan is activated 366 times.